Análisis de cómo se presenta los fraudes electrónicos a través de los sistemas bancarios en las entidades financieras en Colombia para el primer semestre del año 2023

Resumen

El fraude electrónico en Colombia actualmente y en constante avance se está convirtiendo en una afectación con un impacto enorme tanto para las entidades, empresas y usuarios. La tecnología ha avanzado considerablemente y las personas están más atadas a los medios digitales para realizar sus procesos como realizar pagos o trámites. Durante el 2023 se ha evidenciado con más frecuencia ataques, infortunadamente se han generado fraudes por este medio afectando así la integridad del usuario y su economía. A raíz de esta problemática las entidades han tratado de controlar con medidas tecnológicas para garantizar una mayor seguridad, se puede evidenciar en plataformas donde solicita autenticación con más de un factor. No se trata únicamente de fortalecer medidas de seguridad, también es importante que los usuarios estén informados de cómo pueden ser víctimas a través de plataformas, como acceder a información segura y cuales proporcionar. Las entidades pueden complementarlas dando capacitaciones a los usuarios al momento de adquirir obligaciones e inculcando las personas que sean cautelosos al abrir información por medios sospechosos. Según un artículo de la universidad Libre Colombia (2022) menciona que las pérdidas económicas son de aproximadamente seis millones de dólares y el más común es robo de identidad, al mes hay 187 denuncias por robo informático. Tendría un impacto enorme que debe ser tratado desde la identificación y cómo mitigarlo, esto afecta el sector financiero, a los usuarios, empresas y entidades que se encuentran involucrados, esto es un asunto de suma seriedad, se debe generará conciencia al usuario de tener clara los métodos de prevención y sensibilizar de

tener precaución. Es un tema que concierne a toda la sociedad, en cualquier momento puede suceder y se debe exigir a las entidades de prevención que se maneje, debido a que esto procesos algunos pueden ser manejados a nivel nacional.

Palabras claves: cibercrimen, tecnología de la información, Colombia, internet, educación

Introducción

La causa inicial de porque se presentan los fraudes electrónicos en Colombia, tiene como raíz la captación de datos personales con el fin de realizar transacciones fraudulentas, en las cuales, se ve afectado directamente el consumidor y entidad financiera.

La metodología más común utilizada por estos delincuentes es a través de interacciones telefónicas, páginas fachada, enlaces electrónicos y redes sociales, se identifica también que los persuaden sacando información personal y bancaria, muchas veces se hacen pasar por colaboradores del banco y les envían los enlaces para tomar remotamente sus dispositivos electrónicos, también existen puntos de compromisos que estos consisten básicamente cuando hackean la información de una empresa o comercio y los datos que encuentren son intervenidos para saber todo sobre el cliente y ya sabiendo esto llaman al cliente y los engañan fácilmente para vaciar sus productos bancarios.

Según la revista la república recalca que los fraudes digitales han incrementado un 960% en los últimos 3 años donde él informe de omnicanal de Transunion destaca que por el total de las transacciones digitales el 3% es víctima de fraude. En lo anterior se logra relacionar la afectación económica que presentan las entidades financieras por medio de los comercios electrónicos donde a través de diferentes entidades se pueden presentar una

cantidad de transacciones a diferencia de otras donde de igual manera el objetivo es el mismo y la afectación va directamente al consumidor o cliente (Aguilar, 2023).

Malagón (2023), señaló que, a pesar del crecimiento de los delitos informáticos, las transacciones en Colombia son seguras, especialmente las digitales. En Colombia, el 99,99% de las transacciones digitales no tienen reclamaciones por fraude. Esto significa que nuestro sistema digital es seguro que, por ejemplo, jugar Minecraft, el segundo videojuego más popular de la historia. El 0.12% de las descargas de este juego contenían malware y perjudicaron a sus usuarios. En el pensamiento colectivo, hay menos probabilidades de ser víctima de un delito informático jugando que transfiriendo recursos, pero la realidad es otra: nuestro sistema es 11 puntos básicos más seguro que jugar Minecraft, recalcó. (Asobancaria, 2023)

El presidente de Asobancaria enfatizó que, en el sistema financiero local, el 93% de los incidentes cibernéticos no sólo se detectan, sino que se resuelven en menos de un día. En comparación, en Estados Unidos, a pesar de ser una ciber potencia con una infraestructura más avanzada, estos incidentes sólo se detectan en un promedio de 3 días (Asobancaria, 2023)

Además, Malagón mencionó que, a lo largo de este año, el 99,6% de los puntos bancarios no reportaron afectaciones físicas como robos o taquillazos. En la misma línea, reveló que el 99,98% de las transacciones en canales físicos no generaron reclamaciones por fraude. (Asobancaria, 2023)

Es por esto que nos preguntamos ¿Cómo se presentan los fraudes electrónicos a través de los sistemas electrónicos para el primer semestre del año 2023 en Colombia? logrando

desarrollar el siguiente objetivo general se realiza la siguiente descripción como se presenta los fraudes electrónicos a través de los sistemas bancarios en las entidades financieras en Colombia para el primer semestre del año 2023. Relacionando también unos objetivos específicos que ayudarán a Identificar las distintas herramientas de protección de datos para prevenir el fraude en las empresas financieras, describir cómo se catapulta el fraude financiero y cuál es el origen del mismo y Determinar las falencias que presentan las entidades financieras respecto a sus herramientas de prevención de fraude.

Antecedentes

El fraude financiero se ha visto siempre, pero ahora con la llegada de la era tecnológica ha sido un reto para las entidades financieras y el proceso que llevan estas a mantener los productos de los clientes bajo protección de diferentes herramientas, es por esto que se toma como referencia diferentes investigaciones donde establecen la factibilidad del proceso de prevención y detección de fraude electrónico, en donde categorizamos en 3 fases para que su identificación y enfoque sea más factible de comprender.

La detección de fraudes en el sistema financiero

En el artículo “La detección de fraudes de comercio electrónico aplicado a los servicios bancarios (2014)” del autor Fredi Álvarez, podemos identificar de manera clara cuál es el objetivo final para lograr establecer un sistema de seguridad que sea de gran confiabilidad y seguro para los consumidores, esto con el fin de buscar una reducción significativa en las transacciones fraudulentas, y de igual manera se busca lograr entender el algoritmo que se utiliza en dichos procedimientos tanto al iniciar como al terminar el pago.

El artículo de investigación de Jorge Andrés Álvarez Flores y Dora Janeth Preciado Uribe (2022) del Instituto Tecnológico de Antioquia Institución Universitaria busca mejorar la seguridad digital en organizaciones bancarias colombianas para promover la confianza en el entorno digital y mantener la competitividad en el futuro. Adicionalmente el sector bancario ha implementado estrategias anuales para combatir el ciber fraude, como inversiones en tecnología y seguridad digital, colaboración con las autoridades y capacitación en delitos informáticos.

Según el artículo "Fraude al sistema financiero y a sus clientes (2013) " perteneciente a Núñez Ávila Roberto Fabián De la Universidad San Francisco de Quito, nos habla de cuáles son las principales modalidades que se usan para realizar fraudes electrónicos y de igual manera conocer como estas tipologías vienen en aumento al pasar del tiempo, esto con el fin de poder plasmar los procesos y hacer que sea un informe más accesible a los clientes para su respectivo conocimiento y dar un plus a los consumidores financieros para que puedan evitar dichos fraudes y no sean desinformados de las modalidades utilizadas por estas personas.

La protección del consumidor a través del sistema financiero

A través de articulo denominado "la protección del consumidor financiero en Colombia en el uso de los canales electrónicos bancarios (2020)" el cual es estructurado por parte de Celina patricia Amaya perteneciente a la universidad javeriana y en donde se trata de hacer reflexionar al consumidor financiero ante el uso de los canales electrónicos específicamente en Colombia, se logra evidenciar que en la actualidad la mayoría de los consumidores que hace uso de los canales electrónicos, desconocen el proceso y pueden sufrir de fraudes por medio de los mismos, es por eso que la actividad debe hacerse bajo

términos que permitan una verdadera protección en donde se tenga acompañamiento de inicio a fin.

Por medio del artículo “Análisis de la protección al consumidor financiero en las transacciones bancarias en Colombia” realizado por David Zarcos Palacios de la universidad cooperativa de Colombia (2016), se busca establecer de manera legal como están protegidos los consumidores a través de las transacciones bancarias que se realizan en Colombia dando a conocer ciertas leyes las cuales permiten generar confianza y seguridad para el cliente al momento de que realice una transacción y no verse afectado en un fraude electrónico y sin embargo también nos abarca algunas leyes que nos rigen al momento de sufrir un ataque de estas personas maliciosas.

Por medio de la publicación realizada por la Universidad Libre de Colombia en el 2022 por su artículo “protección al Consumidor Dentro del Comercio Electrónico en Colombia” informa que actualmente por la era tecnología mucha de las transacciones, compras o ventas que se hacen por internet hay de por medio información confidencial, por lo que al momento de iniciar estos procesos pueden ser sitios no seguros que aparentan ser de la entidad, por otro lado, también al realizar compras por paginas o redes sociales hay un intermediario para tomar la orden y compra, existen usuarios que por falta de conocimiento brindar información que únicamente deben conocer ellos y no se puede divulgar.

La responsabilidad de las entidades financieras por fraudes electrónicos un articulo originario de Hernández Botero Juliana (2016) en el cual nos da a conocer como cada una de las entidades bancarias debe de hacerse responsable por ciertos procedimientos que se realizan de manera ilegal y de los cuales pasan por alto en la entidad, donde no son detectados o simplemente la seguridad no es la necesaria para poder identificar dicho fraude y

en el cual también nos indica que proceso legal se abarca en este tipo de ocasiones y el derecho que tenemos como consumidor financiero.

El sistema y su análisis en el fraude electrónico

La investigación de Martha Yaneth Ibarra Imbachi (2019) de la Universidad Nacional Abierta y a Distancia se enfoca en delitos informáticos relacionados con ingeniería social en Colombia y Latinoamérica. Muestra deficiencias en la conciencia sobre seguridad de la información y desconocimiento de la ingeniería social, lo que facilita su comisión y estafas. Los ciberdelincuentes emplean tácticas innovadoras que pasan desapercibidas para las víctimas. Destaca la importancia de la capacitación ciudadana para prevenir estos delitos y la responsabilidad de salvaguardar la información financiera al adquirir productos financieros.

En el 2019 la universidad Cooperativa de Colombia publicó un artículo llamado "Análisis del Delito de Fraude Electrónico: Modalidad Tarjeta de Crédito". Esto muestra la importancia de conocer la ley y derechos como usuario a la hora de identificar un fraude electrónico por medio de la tarjeta de crédito. Cuando se inicia un proceso legal por vulneración de información personal y establecer una demanda se debe conocer cómo proceder, debido a que muchas partes están involucradas, como lo son la entidad que suministró la tarjeta de crédito, la entidad que acepta la tarjeta de crédito o el lugar donde se realiza la acción y el ente o individuo que cometió el delito.

Según el artículo publicado por la revista Ibérica de Sistemas e Tecnologías de información en el 2020 "implementación de un Sistema Electrónico de Seguridad Portable para Tarjetas Bancarias" las nuevas tecnologías han permitido que los usuarios puedan realizar operaciones de sus entidades bancarios con mayor seguridad, debido a las nuevas encriptaciones a través de ondas cortas, estas para el usuario son más rápidas y ágiles, por lo

cual, el artículo se basa en que se pueden obtener medidas se seguridad si se entra al mercado y a investigar que pueden proteger sus archivos, igualmente mediante plataformas se pueden obtener herramientas de seguridad para su activación o desactivación de algún producto.

Marco Conceptual.

Si tomamos referencia del origen de los fraudes informáticos se puede retroceder desde los años 60s por el temor infundido por la recolección y almacenamiento de datos personales en computadoras. Éste tiene como referencia la obra "1984" de George Orwell, donde un Gran Hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de tecnologías. Tras la publicación de artículos periodísticos sobre algunos de los casos apareció por primera vez el término delitos informáticos o delincuencia relacionada con computadoras, retomado posteriormente por la literatura fantástica de la época para la publicación de obras relacionadas dentro de un género definido posteriormente como "cyberpunk" (Sain, s.f., parr.2)

Los fraudes electrónicos son actividades ilícitas que involucran el uso de tecnologías de la información y la comunicación para engañar, robar o defraudar a individuos, empresas o instituciones financieras. donde los diferentes tipos de fraudes electrónicos. Los sistemas Bancarios son las infraestructuras tecnológicas y procesos utilizados por las entidades financieras para gestionar sus operaciones y proporcionar servicios a sus clientes y están reguladas por el gobierno colombiano donde ofrecen servicios, como bancos, cooperativas de ahorro y crédito los cuales tiene como componentes de almacenamiento de información llamados servidores, bases de datos, aplicaciones web, aplicaciones móviles, cajeros automáticos, terminales de punto de venta, entre otros,, haciendo énfasis en lo anterior las entidades financieras también están sometidas a tener ataques virtuales por eso se enfoca en

la ciberseguridad y se refiere a las prácticas y medidas para proteger los sistemas informáticos y redes contra amenazas cibernéticas, incluyendo fraudes electrónicos (Electrónico, 2023).

las herramientas como Firewalls, antivirus, sistemas de detección de intrusiones, cifrado de datos y políticas de seguridad, están a la vanguardia y protección de los datos de los cliente de cada una de las empresas en donde estas herramientas controlarán los métodos de Fraude Electrónico y permiten detectar el fraude sin estas habrán consecuencias como Pérdida financiera para los clientes y el mismo banco, daño a la reputación de las entidades, Costos de investigación y mitigación e impacto en la confianza de los clientes. (Grupo Smartekh, 2023)

Dado lo anterior sería ideal la capacitación financiera hacia los clientes informándoles de cómo le puede robar la información personal y bancaria y los métodos más comunes son los siguientes:

> ***Ingeniería social***: "Técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta". (Peña, 2023, pág. 13)

> ***Malware***: "Término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software". (Peña, 2023, p. 13)

Phishing: Este es un tipo de fraude que ocurre a través de plataformas en línea en las que un tercero viola los patrones de seguridad para obtener información valiosa como claves de usuarios bancarios, cuentas bancarias, número de tarjetas de crédito y códigos de autorización para utilizar nuestras herramientas financieras para su beneficio, ellos logran obtener la información por medio malware o virus instalados en los dispositivos dado que los clientes abren links y por medio de estos se conectan remotamente a los dispositivos electrónicos del cliente, computador y teléfono móvil. (Peña, 2023, p. 13)

Pharming: Este modelo más sofisticado consta en la replicación de las estructuras digitales de las entidades bancarias. En este tipo de delitos los usuarios son engañados e ingresan a plataformas que parecen ser las plataformas oficiales de los bancos. Esta usurpación les permite a los delincuentes obtener los datos y tomar control total sobre nuestras finanzas personales. (Peña, 2023, p. 13)

***Sim Swapping*:** Peña, (2023) menciona “Fraude que permite a los criminales robar la identidad mediante el secuestro del número del número de teléfono al obtener un duplicado de la tarjeta SIM Card”. (p. 14)

Hay que tener en cuenta que si no hay una buena estructura tecnológica estos fraudes generan factores de riesgo y habrá una vulnerabilidad en la respuesta de las herramientas y los atacantes pueden explotar como ellos quieran la parte financiera del banco. Es importante enfatizar en los factores humanos como la falta de conciencia de seguridad y la negligencia de los usuarios con esto puede aumentar el riesgo de fraude, el compartir información financiera y personal le dará un boleto gratis al delincuente a que desocupe las cuentas y tarjetas bancarias. (Peña, 2023)

Si trabajamos paralelamente con la evolución de la tecnológica y la curva creciente de herramientas sofisticadas como lo pueden ser métodos de autenticación de ingresos a los portales bancarios y estamos un paso adelante de las tecnologías utilizadas por los atacantes, con estas medidas de Prevención y Detección como el token, implementación de soluciones de ciberseguridad, educación y concientización de los usuarios, monitoreo constante y detección temprana de actividades sospechosas y con el mejoramiento de las herramientas tecnológicas de cada una de las entidades podemos ponerle fin a los fraudes cibernéticos evidenciados en la actualidad. (Peña, 2023)

generando una breve conclusión podemos decir que este marco conceptual proporciona una base sólida para comprender cómo se presentan los fraudes electrónicos a través de los sistemas bancarios en las entidades financieras en Colombia, y puede servir como punto de partida para un análisis más detallado y una estrategia de prevención efectiva.

Marco legal

Es de gran importancia entender como consumidor financiero cuáles son los derechos a los cuales tenemos acceso y cómo estamos protegidos en el sector bancario, es por ello que nos permitimos dar a conocer ciertas normativas en las cuales podemos encontrar cuando aplica cada una de ellas, cuáles son los deberes de las entidades financieras y adicional saber por qué es importante conocer cada una de ellas, con esto podemos evitar ser vulnerados por procesos generados de manera incorrecta y no ser desconocedores de la “norma” como coloquialmente se dice:

Tabla 1

Normativas legales

N° Norma	Orden	Normativa	Indica	¿Por qué es importante?
1	Nacional	LEY 1273 DE 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Es de gran importancia para los colombianos ya que a través de ella se promueve la integridad de los ciudadanos, se abarca en la protección de los datos personales,se promueve la seguridad cibernética y esto hace un entorno más seguro y confiable para la tranquilidad de los consumidores y empresas de colombia.
2	Internacional	Ley N° 21.234	Limita la responsabilidad del usuario de medios de pago y transacciones electrónicas ante el caso de extravío, hurto, robo o fraude.	A través de esta ley se busca la protección del consumidor financiero, en donde se promueve la integridad de las transacciones electrónicas y adicional a

				ello se facilita la denuncia y resolución de estos fraudes cibernéticos.
3	Nacional	Ley 1480 de 2011	Tiene como objetivos proteger, promover y garantizar la efectividad y el libre ejercicio de los derechos de los consumidores, así como amparar el respeto a su dignidad y a sus intereses económicos, en especial, lo referente a: 1. La protección de los consumidores frente a los riesgos para su salud y seguridad.	Esta ley nos garantiza el derecho como consumidores y adicional promueve la transparencia de las transacciones financieras y nos ofrece un mecanismo factible para la resolución de conflictos.
4	Nacional	Ley 599 de 2000	"de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	A través de reformas legislativas, Colombia ha introducido disposiciones que tipifican los delitos informáticos, lo que incluye acciones

				relacionadas con el fraude electrónico y el acceso no autorizado a sistemas informáticos.
5	Nacional	Ley 1328 de 2009	Las entidades vigiladas deberán disponer los recursos financieros para garantizar que el Defensor del Consumidor Financiero cuente con los recursos físicos, humanos, técnicos y tecnológicos y los demás que este considere necesarios, para el adecuado desempeño de sus funciones asignadas.	Se garantiza el uso de los recursos técnicos y tecnológicos para el uso de los sistemas financieros y es importante que un consumidor pueda contar con los recursos necesario para sus transacciones seguras en colombia.
6	Nacional	Ley 1581 de 2012	Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y	Es importante para el ciudadano como para el consumidor financiero tener la seguridad y confianza de que sus datos personales son salvaguardados de manera segura y que no

			garantías constitucionales a que se refiere el artículo 15 de la Constitución Política.	sea de conocimiento para todos.
7	Nacional	Circular 052 de 2007	Se establece la necesidad de que los canales de intercambio de información entre entidades financieras y sus clientes cumplan con criterios básicos de seguridad y calidad en el manejo de la información. Se destaca la necesidad de satisfacer los atributos de confiabilidad e integridad.	Permite brindar la confianza a los colombianos en que los canales transaccionales que usamos para nuestros temas bancarios sean seguros y cuenten con una excelente calidad en el manejo de la información.
8	Nacional	Circular Externa 008 de 2018	Imparte instrucciones en materia de requerimientos mínimos de seguridad y calidad para la realización de operaciones.	Obliga a las entidades a cumplir con los requerimientos mínimos para el tema de las transacciones en las pasarelas de pago y con ello el consumidor estar tranquilo en un proceso adecuado y seguro dentro

				del mismo sistema.

Nota: Esta tabla nos muestra varias de las leyes y normas más importantes en el tema a tratar, nos indica su tipo de orden, la normativa dada, lo que indica textualmente cada una de ellas y el porqué es importante el conocimiento de la misma.

Reflexión

El fraude electrónico en los sistemas bancarios de Colombia, como en cualquier parte del mundo, nos ha presentado una serie de desafíos y reflexiones importantes y tiene como causa y efecto generar la responsabilidad compartida, es decir, en este mundo, los bancos y las entidades financieras tienen un papel crucial en la protección de los datos y activos de los clientes o consumidores. Se han implementado una serie de medidas de seguridad, como la autenticación de dos factores y el monitoreo de transacciones y todo esto para poder mitigar los riesgos. Sin embargo, los clientes también deben asumir la responsabilidad de proteger sus propios activos financieros. Esto implica tomar medidas para proteger contraseñas y datos personales, así como educarse sobre las amenazas cibernéticas y ser conscientes de las prácticas seguras en línea ya que muchos tal vez por el mismo desconocimiento generan procesos desconocidos o que para ellos son “Normales” cuando no es así y son víctimas de estos delincuentes.

Adicional a ello Hernández Botero, J. (2020) nos indica que en Colombia los consumidores financieros tienen la oportunidad de señalar condiciones y reglas para la utilización de sus productos financieros en donde se puede por voluntad propia determinar como es el uso de sus canales electrónicos, la cantidad de transacciones , el tope y demás limitantes que ayudan a poder mitigar un poco el fraude electrónico en donde también se

resalta la importancia de la colaboración entre las partes interesadas. Las instituciones financieras, las autoridades gubernamentales y las empresas de ciberseguridad deben trabajar juntas para compartir información y estrategias para contrarrestar las amenazas cibernéticas ya que esto es de gran importancia para que no se pueda ampliar en gran escala los ataques producidos y mitigar en gran porcentaje la afectación en los consumidores ya que al final son ellos los más impactados por estos ataques y que sin embargo tampoco deben ser quienes no aporten o de su contribución al proceso ya que son los que ayudan principalmente con su conocimiento a cerrar las puertas a dichos delincuentes.

A medida que la sociedad se adentra cada vez más en la era tecnológica, las vidas de las personas y los recursos financieros están completamente vinculados a la tecnología. Esto ha generado oportunidades sin precedentes para la eficiencia y la comodidad, pero también ha abierto la puerta a nuevas formas de delincuencia, como el fraude electrónico y muchas personas se han visto afectadas por ello.

Uno de los aspectos más notables de estos incidentes, es la creciente intensidad de los ataques cibernéticos. Los atacantes detrás de estos fraudes demuestran una habilidad y creatividad para realizar sus fechorías. Utilizan tácticas como la técnica de la persuasión y por medio de los fraudes como el phishing, el malware bancario y demás métodos para engañar a los usuarios y obtener acceso a sus cuentas. Esta evolución constante nos recuerda que, en un mundo digital, la ciberseguridad nunca puede ser estática. La defensa contra el fraude electrónico requiere una adaptación constante y un esfuerzo conjunto entre instituciones financieras, reguladores y los mismos consumidores para poder abarcar un sistema de defensa hacia ellos.

Saade, C. P. A. (2020). Protección del consumidor financiero en Colombia en el uso de canales electrónicos bancarios. Universitos, 69, 123-145. La Ley 1328 de 2009 en Colombia y las iniciativas internacionales promueven la "alfabetización financiera y el empoderamiento del consumidor". Esto implica que los consumidores deben ser educados y empoderados para comprender los riesgos y beneficios de los productos y servicios financieros que utilizan. Además, se destaca la función de la Superintendencia Financiera de Colombia en la protección del consumidor financiero y su capacidad para abordar quejas y conflictos de manera ágil y efectiva.

para las entidades bancaria es importante que cuenten con una infraestructura digital y que las herramientas que se utilicen sean de gran eficiencia para el control del fraude como lo pueden ser Sistemas cognitivos e inteligencia artificial, Sistemas contables distribuidos particularmente en pagos y tarjetas de crédito, Sistemas basados en tecnología de Blockchain que permiten asegurar la inmutabilidad de datos, utilizando hash criptográficos, Herramientas de autenticación biométrica con el fin de debilitar riesgos relacionados con robo de identidad, Herramientas de autenticación biométrica, autenticación con base en geolocalización, así como claves criptográficas que garanticen que la operación de los sistemas de pago de las empresas que ofrecen este servicio no es propensa a sufrir fraude o violación de datos, modelos de análisis de comportamiento con el fin de realizar continuos procesos de monitoreo para prevención de fraude y automatización de procesos y aprendizaje de máquina para detectar y prevenir fraudes electrónicos.

En última instancia, el fraude electrónico es un recordatorio de que, en este mundo cada vez más digital y en donde prácticamente vivimos una revolución nueva, la seguridad no es un lujo, sino una necesidad. Los incidentes de fraude electrónico nos llevan a mantener un

equilibrio entre aprovechar los beneficios de la tecnología y proteger nuestros activos financieros y datos personales.

La reflexión más destacada que se deriva de estos incidentes es que la ciberseguridad es una responsabilidad compartida que requiere vigilancia constante, educación y colaboración. La tecnología continuará evolucionando y con ella las amenazas cibernéticas. Para garantizar un sistema bancario seguro en Colombia y en cualquier parte del mundo, debemos estar preparados para adaptarnos y protegernos en un entorno digital en constante cambio.

Conclusiones

La presente investigación se adentró en el complejo panorama de los fraudes electrónicos en las entidades financieras de Colombia durante los últimos años y principalmente para el primer semestre del año 2023. El análisis exhaustivo de este tema, en donde se puede identificar de gran manera la necesidad de fortalecer las defensas y comprender mejor las amenazas que rodean a las instituciones financieras en la era digital. A lo largo de esta investigación, hemos alcanzado una serie de conclusiones significativas que resumen los hallazgos y los puntos clave de este estudio.

En primer lugar, se lograron identificar diversas formas y herramientas de protección de datos que desempeñan un papel fundamental en la prevención de fraudes en las diferentes empresas financieras. Estas herramientas abarcan desde sistemas avanzados de autenticación y encriptación de datos, hasta técnicas de detección de anomalías y monitoreo constante de transacciones. Sin embargo, es esencial destacar que la efectividad de estas herramientas depende de una implementación adecuada y su actualización constante para hacer frente a las maneras cambiantes de los delincuentes cibernéticos que intentan hacer daño a la sociedad.

En segundo lugar, se exploró el origen del fraude financiero y se evidenció que, en la mayoría de los casos, proviene de la combinación de factores como la ingeniería sistemática, la vulnerabilidad de sistemas que ya son obsoletos y la falta de conciencia en materia de seguridad por parte de los usuarios. Es necesario que las entidades financieras tomen medidas las cuales sirvan para educar a sus clientes y empleados sobre las amenazas en constante evolución y de esta manera poder fomentar una cultura de seguridad a través de los sistemas bancarios.

En tercer lugar, se llegaron a determinar algunas de las falencias que presentan las entidades financieras en relación con sus herramientas de prevención de fraude. Estas deficiencias pueden atribuirse a la falta de inversión en tecnologías de respaldo, la resistencia al cambio, la falta de capacitación y la subestimación de la amenaza del fraude electrónico. Para abordar estas debilidades que se tienen, es necesario que las instituciones financieras realicen auditorías de seguridad muy frecuentemente y que adicional se establezcan en un plan integral de seguridad cibernética.

Referencias

Aguilar, k. V. (18 de ABRIL de 2023). LA REPUBLICA. Obtenido de https://www.larepublica.co/finanzas/los-intentos-de-fraude-digital-en-colombia-han-crecido-859-en-los-ultimos-tres-anos-3594974

Asobancaria. (26 de octubre de 2023). *En Colombia, más del 99% de las transacciones financieras, tanto digitales como físicas, se realizan sin incidentes de fraude*. Obtenido de asobancaria: https://www.asobancaria.com/2023/10/26/en-colombia-mas-del-99-de-las-transacciones-financieras-tanto-digitales-como-fisicas-se-realizan-sin-incidentes-de-fraude/

Electronico, F. (2023 de junio de 2023). *Canal Institucional*. Obtenido de Canal Institucional: https://www.canalinstitucional.tv/te-interesa/fraude-electronico-recomendaciones-evitar-estafas-en-linea#:~:text=El%20fraude%20electr%C3%B3nico%20se%20refiere,encuentran%20principalmente%20los%20fines%20econ%C3%B3micos.

Grupo Smartekh. (07 de julio de 2023). *Linkedin*. Obtenido de Linkedin: https://es.linkedin.com/pulse/nuevas-tecnolog%C3%ADas-y-soluciones-de-seguridad-mejorando-la-defensa

Peña, D. A. (2021 de junio de 2023). *CIBERSEGURIDAD DE LA IDENTIDAD DIGITAL EN LAS TRANSACCIONES ELECTRÓNICAS BANCARIAS EN COLOMBIA [version PDF]*. Obtenido de Repositorio aianstitucional UNAD: https://repository.unad.edu.co/handle/10596/56866

Sain, G. (s.f.). Evolución histórica de los delitos informáticos.

Moreno, J, C., Sánchez, C. S., Salavarrieta, J. C., Vargas. L,M.,(2019). Soluciones Tecnológicas para la Prevención de Fraude y diseño de un Modelo de Prevención del Riesgo Transaccional para el Botón de Pago. Scielo. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672019000200036

Mora Aguilar, k., (2023). Los intentos de fraude digital en Colombia han crecido 859% en los últimos tres años. La Republica https://www.larepublica.co/finanzas/los-intentos-de-fraude-digital-en-colombia-han-crecido-859-en-los-ultimos-tres-anos-3594974

Rodríguez Zarate, A., (2014). análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos: el riesgo provecho, el riesgo creado y el riesgo profesional.

Cielo. http://www.scielo.org.co/scielo.php?pid=S0041-90602014000100010&script=sci_arttext

Álvarez Flórez, J. A., Preciado Uribe, D. J. (2021). Evolución del fraude informático: una problemática en las organizaciones bancarias colombianas.

Ibarra Imbachi, M. Y. Delitos informáticos asociados a la ingeniería social en Colombia y Latinoamérica.https://repository.unad.edu.co/bitstream/handle/10596/27420/%20%09myibarrai.pdf?sequence=1&isAllowed=y

Celina Patricia Anaya Saade, Universidad del Magdalena, Santa Marta, Colombia https://revistas.javeriana.edu.co/index.php/vnijuri/article/view/30215

David Zarco Palacios, Santa Marta – Colombia (2016). https://repository.ucc.edu.co/items/1d3320c3-0654-4ace-bb69-624cfac7915b

Fecha 2020 Autor Hernández Botero Juliana, https://repository.upb.edu.co/handle/20.500.11912/6161